☑ Original ❒ Du

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A 2016 red Ford Focus, Wisconsin license plate 877LWJ, VIN 1FADP3F24GL274453

Case No. 22-M-599 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A-3

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 11-14-22 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 10-31-22 9:05 am

Stephen C. Dri
Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-3

DESCRIPTION OF PROPERTY/LOCATIONS TO BE SEARCHED

1. A 2016 red Ford Focus, Wisconsin license plate 877LWJ, VIN 1FADP3F24GL274453.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense; contraband; the fruits of crime; or property designed, or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2251(a)(2), and Title 18, United States Code, Section 2422(a):

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting,

through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of

names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

    h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone. Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the

camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A 2016 red Ford Focus, Wisconsin license plate 877LWJ, VIN 1FADP3F24GL274453

Case No. 22-M-599 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A(a)(2)	Receive and distribute child pornography
18 U.S.C. 2252(a)(5)(B)	Posses, or knowingly access with intent to view child pornography

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Timothy Kastner, FBI TFO
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 10-31-22

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Timothy Kastner, having been first duly sworn, depose and state as follows:

INTRODUCTION

1. I am currently employed as a Detective for the Wauwatosa Police Department. I have been employed as a law enforcement officer for over twenty-one years. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) and have been so since June 2021. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division, and I am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the distribution of child sexual abuse material.

2. I have received training to investigate child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review, as well as sophisticated techniques used to commit cybercrimes

3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable. Some of the information was provided in response to administrative subpoenas and I believe this information to be also be reliable.

4. Based upon the information described below, I submit that probable cause exists to believe that the subject, Jordan JC Simon DOB 11/25/97, residing at 5228 N 108 Court, Milwaukee, Wisconsin 53225 (SUBJECT PREMISES), utilizing the Snapchat account "les_m2020" (TARGET ACCOUNT) has committed the crimes of Possession of Child Pornography and Distribution of Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(2) and in violation of Title 18, United States Code, Section 2252(a)(5)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the SUBJECT PREMISES; inside a 2016 red Ford Focus with Wisconsin license plate 877LWJ; and on Jordan Simon's person; more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a hand-held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving,

and storing text messages and e-mails; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer Server" or "Server," is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. "An Internet Protocol address" (IP address) is a unique alphanumeric address used by internet-enabled electronic storage devices to access the Internet. Every electronic

storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I have consulted in this matter with law enforcement personnel and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. Through this consultation, I learned that to properly retrieve and analyze electronically stored computer data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To achieve such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

7. Based on my knowledge, training, and experience, and consultation with forensically trained FBI personnel, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;
b. The objects may have been used to collect and store information about crimes (in the form of electronic data); and
c. The objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device and storage media in particular, computers internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture,

and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either

inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

10. Based upon my knowledge, training and experience, and consultation with forensically trained personnel, I know that a thorough search for information stored in storage media often requires law enforcement to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

11. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the law enforcement personnel executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

12. I know that when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain: data that is evidence of how the electronic storage

device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

BACKGROUND ON OMEGLE

13. Omegle is a free online chat website that allows users to socialize with others without the need to register or create an account. The service randomly pairs users in one-on-one chat sessions where they chat anonymously. Omegle does not retain the content of the chats on their platform. The Omegle platform is known by law enforcement to be used by child predators to meet and exploit children online. Omegle is also known by law enforcement to be a means for those who collect and distribute Child Sexual Abuse Material to meet and connect.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

14. As explained below, the user of the Snapchat account "les_m2020", used the account on numerous occasions to distribute and receive child pornography to a number of different users on Snapchat.

15. On February 19, 2022, US Citizen Kaitlyn Martinez reported to the Federal Bureau of Investigation (FBI) that she used the chat function on the website Omegle on 02/19/22 to connect to and chat with a random stranger. While chatting with the stranger, the stranger asked Martinez if she wanted "CP". Martinez was unsure what CP meant and told the person yes. The stranger provided Martinez with a Snapchat username of "les_m2020" and told Martinez to chat with them on Snapchat.

16. Through my training and experience, I know "CP" to be an abbreviation for Child Pornography.

17. Martinez then used her own Snapchat account, with username "Kait.lyn0528", to continue to chat with the stranger at Snapchat account "les_m2020". The stranger sent Martinez three MEGA links through Snapchat's chat function. Martinez opened one of the links and it directed her to a library of pornographic videos. Martinez viewed some of the videos and recognized that they contained children, some of whom were pre-teen, engaged in sexually explicit conduct.

18. On March 04, 2022, Martinez provided written consent to FBI to download the content of her Snapchat account with username "Kait.lyn0528" as well as to view her chat with "les_m2020" that was saved within her account.

19. I downloaded and viewed the Snapchat chat messages between "Kait.lyn0528" and "les_m2020". The chat conversation began on 02/19/22 at 2:25am and ended on 02/19/22 at 2:45am. The chat conversation is as follows:

2022-02-19 02:25:25am	les_m2020: hey
2022-02-19 02:25:47am	Kait.lyn0528: hey
2022-02-19 02:26:21am	les_m2020: Can you send a live to verify youre a girl?
2022-02-19 02:26:58am	les_m2020: Very Cute
2022-02-19 02:27:02am	Kait.lyn0528: Haha thanks
2022-02-19 02:27:06am	les_m2020: (MEGA link ending 96hZYg)
2022-02-19 02:27:14am	les_m2020: Theres the omegle
2022-02-19 02:27:23am	les_m2020: (MEGA link ending 5ClW0Jil)
2022-02-19 02:27:38am	les_m2020: Telegram/of
2022-02-19 02:28:33am	les_m2020: I have more cp

2022-02-19 02:28:53am	les_m2020: (MEGA link ending ShQtbucwWqGA)
2022-02-19 02:30:28am	les_m2020: Few more links, youll have to send for the rest
2022-02-19 02:39:09am	les_m2020: Like them?
2022-02-19 02:44:00am	Kait.lyn0528: Where did you get all this?
2022-02-19 02:44:44am	les_m2020: From trading on omegle
2022-02-19 02:45:21am	Kait.lyn0528: Oh
2022-02-19 02:45:56am	les_m2020: Would you snap for more?

20. I observed that "les_m2020" sent three MEGA links within the chat conversation. I viewed the content of those three MEGA links. One of the links, ending "ShQtbucwWqGA", contained 20 Child Sexual Abuse files, including:

a. Filename: !!!ibs....

This 54 second video depicts a topless pubescent age female with her breasts exposed, kneeling in front of a young pre-pubescent boy, 3-5 years old. The female pulls down the pants and underwear of the boy, exposing his penis. The female sexually assaults the boy with mouth to penis contact.

b. Filename: 3E2BB3C2-F62A-4AF0-BCBC.....

This video is 5 minutes and 41 seconds long. The camera is zoomed in on the vagina of a young pre-pubescent girl, 3-6 years old. The girl is lying on her back with an adult male in between her legs. The man is sexually assaulting the girl with penis to vagina penetration. The man also makes mouth to vagina contact with the girl.

c. Filename: 5EBFB490-33A3-43DB-B166.....

This 50 second video depicts a toddler aged female child, 1-3 years old, nude and lying on her back. A nude adult male is in between the child's legs and sexually assaulting her with finger to vagina contact, penis to anus contact, and penis to pubic area contact.

d. Filename 698D00C1-A1C4-42D6-AB43.....

This 31 second video depicts a young pre-pubescent girl, 4-7 years old, nude and lying on her back on a couch. There is a nude adult male in between the girl's legs who is sexually assaulting her with penis to vagina penetration.

e. Filename 5772B28E-58E7-4360-9B71.....

This 1 minute 20 second video depicts a nude adult male standing in front of a young toddler child, 2-3 years old, who is wearing pajamas. The male sexually assaults the child with penis to mouth contact.

21. On March 04, 2022, an administrative subpoena was served to Snap Inc. for subscriber and IP information associated to the username "les_m2020". On March 14, 2022, Snap Inc. responded to the subpoena and identified the username "les_m2020" as being registered with the email address of ojibwa7@gmail.com. Snap Inc. provided that the "les_m2020" account was created on January 02, 2020, at 02:00:18 UTC by a user connected to Snapchat using the IP address 174.82.249.131, which resolved to Spectrum, owned by Charter Communications.

22. On March 16, 2022, an administrative subpoena was served to Charter

Communications for subscriber information associated to the account using IP address 174.82.249.131 on January 02, 2020, at 02:00:18 UTC. On March 31, 2022, Charter Communications responded and provided the following information:

Subscriber Name: Jeff Simon

Subscriber Address: 2829 Long Valley Rd, Richfield, WI 53076

23. On May 6, 2022, an administrative subpoena was issued to Google Inc for the subscriber details and IP logs of account ojibwa7@gmail.com. On May 7, 2022, Google Inc provided that the subscriber name was **Jordan Simon** and recovery phone number was 414-750-6647. There were 5 credit cards linked to the account, all in the name **Jordan Simon**. The billing information for the account was **Jordan Simon**, 2829 Long Valley Rd, Richfield, WI 53076, phone 414-750-6647. The IP logs showed logins to the google account from IP address 174.82.145.141 between February and May 2022.

24. On May 6, 2022, a search warrant for the content of Snapchat account "les_m2020" was obtained in the United States District Court for the Eastern District of Wisconsin. The contents discussed in subsequent paragraphs were obtained from Snap Inc. in the results of the search warrant. I have reviewed the contents of the return provided by Snap Inc.

25. Within the Snapchat records for account "les_m2020", in addition to the email address ojibwa7@gmail.com, there were 2 other email addresses linked to the account. The additional linked emails were lesm2020lesm2020@gmail.com, added on 01/30/2022, and lesomgfun@gmail.com, added on 01/31/2022.

26. Within the Snapchat records for account "les_m2020" there was additional evidence of possession, receipt, and distribution of child pornography, detailed below.

27. On 02/18/22 and 03/02/22, “les_m2020” sent the same MEGA link ending “ShQtbucwWqGA”, that was sent to “Kait.lyn0528” and contained the previously described Child Sexual Abuse Material, to three other Snapchat users.

28. On 03/02/22, “les_m2020” received a video file showing a female child, 4-7 years old, being sexually assaulted by a man with penis to mouth contact.

29. On 03/22/22, “les_m2020” received a video file showing a person sexually assaulting a female child, 4-9 years old, by making hand to vagina contact with the child.

30. Between 03/14/22 and 04/24/22, “les_m2020” sent a video file of a female child 6-10 years old, being sexually assaulted by a man with penis to mouth contact, to five different snapchat users.

31. On 03/14/22 and 03/19/22, “les_m2020” sent a video file of a female child, 7-11 years old, who is nude and inserting a toothbrush into her vagina, to two different snapchat users.

32. On 03/19/22 and 05/03/22, “les_m2020” sent a video file of a female child, 7-11 years old, being sexually assaulted by a man with penis to mouth contact, to two different snapchat users.

33. Within the Snapchat records for “les_m2020”, the login IP address of 174.82.145.141 was captured first used on 04/09/22 at 21:23:04 UTC and last seen on 05/09/22 at 11:40:52 UTC. This was the same IP address used to login to Google account ojibwa7@gmail.com on numerous days between 02/05/22 and 05/04/22.

34. On June 8, 2022, an administrative subpoena was issued to Charter Communications for IP 174.82.145.141 on 04/09/22 and 05/09/22. On June 13, 2022, Charter

Communication provided that the subscriber was Jeff Simon at 2829 Long Valley Rd, Richfield, WI 50376.

35. On July 13, 2022, an administrative subpoena was issued to US Cellular for subscriber information for the cell phone number 414-750-6647. On July 14, 2022, US Cellular provided that the subscriber is Patricia Simon at 2829 Long Valley Rd, Richfield, WI 53076. There are five cell phone numbers linked to Patricia Simon's US Cellular account, indicative of a "family plan". The device associated to cell phone number 414-750-6647 is a Samsung Galaxy S10 with IMEI 35818010115449.

36. A WI Department of Transportation records check for **Jordan JC Simon DOB 11/25/1997** shows his address on his driver's license file is 2829 Long Valley Rd, Richfield WI 53076. I viewed the DOT photograph of Jordan Simon.

37. An employment history of Jordan Simon was requested from Wisconsin Department of Workforce Development and the records showed Jordan Simon's most recent employer was Harley Davidson Motor Company.

38. A Facebook account for Jordan Simon was located and it shows his employer is Harley Davidson and his father is Jeff Simon. The Facebook page for Jeff Simon shows he is married to Patty Simon. A review of Patty Simon's Facebook page revealed a post with photos of Jordan Simon referencing Jordan as Patty's son.

39. A Transunion TLOxp records check for the phone number 414-750-6647 showed that it was associated to **Jordan JC Simon** at 2829 Long Valley Rd, Richfield, WI.

40. An Experian records check for the phone number 414-750-6647 showed that it was associated to **Jordan J Simon** at 2829 Long Valley Rd, Richfield, WI.

41. On August 5, 2022, a search warrant was obtained for additional records of the Google account ojibwa7@gmail.com. On August 10, 2022, Google provided records that showed the ojibwa7@gmail account was accessed from the following Spectrum IP addresses:

a. IP 72.133.205.210 on 06/13/22 and 06/16/22

b. IP 74.135.177.143, nine times between 06/18/22 and 07/06/22

c. IP 72.133.200.250 on 07/11/22 and 07/15/22

42. On September 6, 2022, an administrative subpoena was issued to Spectrum/Charter Communications for the IP addresses in paragraph 41 at the dates and times they were utilized by the ojibwa7@gmail account. On September 9, 2022, Spectrum/Charter provided that all three IP addresses resolved to:

a. Subscriber: Patricia Simon

b. Service location: **5228 N 108 Ct, Milwaukee, WI 53225**

43. Physical surveillance was conducted at **5228 N 108 Ct, Milwaukee WI 53225**. On 07/13/22 at 6:28am, **Jordan Simon** was observed arriving to the residence in a **red Ford Focus with WI license plate 877LWJ**. Jordan Simon parked the Ford on the street in front of the residence and entered the duplex through the side (south) door.

44. On 07/14/22 at 6:24am, during physical surveillance, **Jordan Simon** was observed leaving Harley Davidson, W156 N9000 Pilgrim Rd, Menomonee Falls, WI in the same **red Ford with WI plate 877LWJ**. Simon drove the Ford to **5228 N 108 Ct, Milwaukee WI**, parked on the street, and went into the duplex.

45. The physical surveillance at **5228 N 108 Ct**, **Milwaukee, WI** between July 2022 and October 2022 indicates that additional members of the Simon's family are also living at the residence and/or have regular access to it.

a. On 07/13/22 at approximately 6:30am, Jordan Simon's sister Amy Simon left the residence in a white Ford with WI plate 949XFE. The white Ford was later located at Froedtert Menomonee Falls Hospital, where Amy Simon is employed. The white Ford has been observed at the residence regularly during surveillance and it has not been observed at 2829 Long Valley Rd, Richfield WI. The listed owner of the white Ford is Amy's father Jeffrey C Simon.

b. On 07/13/22 at approximately 5:30am, Jordan Simon's mother, Patricia Simon, was observed leaving the residence in a red Ford hatchback with WI plate705ERG. The red Ford hatchback was later located at Ascension SE WI at 201 N Mayfair Rd, Wauwatosa WI, where Patricia is employed. The red Ford hatchback has been observed at the residence regularly during surveillance and it has not been observed at 2829 Long Valley Rd, Richfield, WI. Patricia Simon has also been observed on the balcony of the upper unit at 5228 N 108 Ct, Milwaukee, smoking cigarettes on numerous occasions. The listed owners of the red Ford hatchback are **Jordan JC Simon** and Jeffrey Simon.

c. On 09/27/22 at approximately 4:20pm, a red Ford Explorer with WI plates AJP2049 was parked on the street in front of the residence. This Ford Explorer has been observed in the driveway of the residence on numerous prior occasions. The listed owner of the Ford Explorer is Amy S Simon and Jeffery C Simon.

46. A WI Department of Transportation records check on the WI license plate **877LWJ**

revealed that the it is registered to a **2016 red Ford Focus, VIN 1FADP3F24GL274453**, and the owners are **Jordan JC Simon DOB 11/25/97** and Jeffery C Simon DOB 08/08/64 with an address on file of 2829 Long Valley Rd, Richfield WI.

47. A search warrant was obtained for cell phone records for phone number 414-750-6647 and upon receipt of the location data, it was analyzed and mapped. The location data shows that prior to June 2022, the top cell tower used by phone number 414-750-6647 was 0.4 miles from 2829 Long Valley Rd, Richfield, WI. Within the month of June 2022, the top cell tower used by phone number 414-750-6647 switched to a tower 0.89 miles from **5228 N 108 Ct, Milwaukee, WI**. **The change in top cell tower location is indicative of the user moving to a new residence**.

48. The cell phone records for 414-750-6647 also show regular usage during the overnight hours in the area of Harley Davidson at W156 N9000 Pilgrim Rd, Menomonee Falls, WI. The cell phone location records are indicative of the user working third shift at Harley Davidson.

49. A check of publicly available City of Milwaukee tax assessor records shows that the owners of the duplex at **5226/5228 N 108 Ct, Milwaukee, WI 53225** is Jeffery C Simon and Patricia A Simon with an address on file of 2829 Long Valley Rd, Richfield, WI.

50. Additional physical surveillance at **5228 N 108 Ct. Milwaukee, WI** has resulted in observations of the **red Ford Focus with WI plate 877LWJ**, which is known to be driven by Jordan JC Simon, regularly parked on the street in front of the residence at various times of day throughout September 2022. On 09/22/22 at 9:59pm, I observed a white male I recognized to be **Jordan Simon** exit the side door of the residence and get into his **red Ford Focus WI plate 877LWJ** and leave.

51. On 10/06/22, during physical surveillance, **Jordan Simon** was observed leaving Harley Davidson, W156 N9000 Pilgrim Rd, Menomonee Falls, WI in the **red Ford with WI plate 877LWJ**. Simon drove the Ford to **5228 N 108 Ct, Milwaukee WI** and then went into the residence.

52. On 09/22/22, a utilities inquiry was made to WE Energies for the duplex at 5226 / 5228 N 108 Ct, Milwaukee WI, 53225. WE Energies provided that the upper unit of **5228 N 108 Ct, Milwaukee WI 53225** is in customer name Patricia Simon and was activated on **06/03/22**. WE Energies provided that the lower unit of 5226 N 108 Ct Milwaukee is in customer name James Jones and was activated 06/15/20.

53. On 09/23/22, the United States Post Office Inspection Service audited the mail to be delivered to 5228 N 108 Ct, Milwaukee, WI, and there was one piece of US mail addressed to **Jordan Simon**. The USPS Inspector confirmed that 5228 N 108 Ct is the upper unit of the duplex at 5226 /5228 N 108 Ct, Milwaukee WI.

54. Through my training and experience, I am aware that Snapchat is a social networking app that is used primarily on mobile devices such as cell phones and tablets. Therefore, the digital evidence associated to the TARGET ACCOUNT is likely to be located on the digital devices owned and utilized by the user.

55. Based on training and experience, I know cellular telephones users typically keep those devices on their person or within close proximity to their person at most times of day and night. I also know that when cellular telephone users are driving a vehicle, they frequently place their cellular telephones within the passenger compartment of the vehicle so they are more readily

accessible to make and receive phone calls or messages, to use navigation features, or to interact with a variety of other mobile applications.

56. Based on training and experience, I also know people regularly maintain or temporarily store personal records, including utility and telephone bills, mail envelopes, addressed correspondence, insurance cards, and vehicle registrations, as well as records, information, and items relating to the ownership or use of their personal electronic devices, including sales receipts, bills for internet access, and handwritten notes, within their vehicles.

Identification of SUBJECT PREMISES

57. The most recent login data available, from June and July 2022, to the Google account ojibwa7@gmail.com, which is the email address linked to both the target Snapchat account "les_m2020" and **Jordan Simon**, show that the Google account was regularly used from IP addresses that resolve to **5228 N 108 Ct, Milwaukee, WI 53225**.

58. The US Cellular tower records for 414-750-6647, which is the phone number associated to **Jordan Simon**, show that the user's top cell tower moved from Richfield WI to the area of **5228 N 108 Ct, Milwaukee WI 53225** in early June 2022.

59. WE Energies utility records show that new utility service was activated 06/03/22 at **5228 N 108 Ct, Milwaukee, WI 53225**, in the name Patricia Simon, whom is Jordan Simon's mother.

60. Employment records obtained showed that **Jordan Simon** worked at Harley Davidson. On July 14, 2022, at approximately 5:45 a.m., I observed Jordan Simon's vehicle, a red Ford Focus with WI license plate 877LJW, in the parking lot at Harley Davidson in Menomonee Falls, WI.

61. On July 14, 2022, at approximately 6:17 a.m., I observed a white male subject I recognized to be **Jordan Simon**, exit the Harley Davidson building in Menomonee Falls and enter his red Ford Focus with WI license plate 877LWJ. Simon drove the Ford Focus to **5228 N 108 Ct, Milwaukee WI 53225** and parked the Ford on the street in front of the residence. Simon exited the Ford an entered the residence.

62. On 09/23/22, a check of the US mail at **5228 N 108 Ct, Milwaukee, WI**, revealed mail to the residence addressed to **Jordan Simon.**

63. Based upon this information there is probable cause to believe that **Jordan Simon** was the user of the TARGET ACCOUNT, and that **Jordan Simon** is residing at the SUBJECT PREMISES. There is probable cause to believe that **Jordan Simon** still resides at the SUBJECT PREMISES and his electronic devices containing further evidence of violations of federal law could be found there.

64. This application seeks permission to execute the search warrant on the person of **Jordan Simon** and the **red Ford Focus with WI plate 877LWJ**, whether they are located at the SUBJECT PREMISES or located elsewhere within the jurisdiction of the court. It is anticipated that the person of **Jordan Simon** and the **red Ford Focus with WI plate 877LWJ** will be located at Harley Davidson, W156 N9000 Pilgrim Rd, Menomonee Falls, WI 53051, and the search warrant of the person and vehicle will be executed there.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

65. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, knowledge, and discussion with other FBI and law enforcement personnel I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps, such as Snapchat, consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

66. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their residences, attached or detached garages, associated outbuildings, their vehicles, or, at times, on their person, and/or other secure locations which they maintain dominion and control of, for ready access and to conceal these items from law enforcement, family members, or other individuals who frequent these areas. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residences, attached or detached garages, associated outbuildings, their vehicles, or, at times, on their person, and/or other secure locations, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

devices).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

67. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

68. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

69. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. I submit there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information

allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a

computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

70. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

71. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

BIOMETRIC ACCESS TO DEVICES

72. This warrant permits law enforcement to compel residents of the SUBJECT PREMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, I believe one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Jordan Simon or other SUBJECT PREMISES's residents to the fingerprint scanner of the devices; (2) hold the devices found in front of the face of Jordan Simon or other SUBJECT PREMISES's residents and activate the facial recognition feature; and/or (3) hold the devices found in front of the face of Jordan Simon or other SUBJECT PREMISES's residents and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel Jordan Simon or other SUBJECT PREMISES's residents state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel Jordan Simon or other SUBJECT PREMISES's residents to identify the specific biometric

characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

Based on the foregoing, there is probable cause to believe that Jordan JC Simon is utilizing or has utilized the Snapchat username "les_m2020" in violation of Title 18 U.S.C. § 2252, which, among other things, makes it a federal crime for any person to possess, receive, or distribute child pornography, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the Premises, inside a red Ford Focus with Wisconsin license plate 877LWJ, and/or on the person of Jordan JC Simons, as described in Attachments A.

ATTACHMENT A-3

DESCRIPTION OF PROPERTY/LOCATIONS TO BE SEARCHED

1. A 2016 red Ford Focus, Wisconsin license plate 877LWJ, VIN 1FADP3F24GL274453.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense; contraband; the fruits of crime; or property designed, or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2251(a)(2), and Title 18, United States Code, Section 2422(a):

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting,

through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of

names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

    h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone. Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the

camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.